

  
**CONECTANDO**  
TERRITORIOS

UN  
PROYECTO  
DE:   
**país**  
digital

# Ciudadano Digital





País Digital promueve el acceso y uso de los servicios de telecomunicaciones y de las tecnologías de información y comunicación (TIC), para mejorar la calidad de vida y las oportunidades de desarrollo de Chile. En ese sentido buscamos guiarte en la consulta, solicitud y gestión de trámites online para el pleno ejercicio de tus derechos digitales.

Este manual consultivo nace en el marco del programa Conectando Territorios y forma parte de un conjunto de tres ejemplares: **Aprendiz Digital**, **Ciudadano Digital** y **Simbiosis Cibernética**. Cada publicación está especialmente diseñada para complementar tu formación en el programa de **Alfabetización Digital**. Esperamos que estos recursos te guíen y motiven tu camino en el fascinante y siempre evolutivo mundo digital. ¡Éxito!

# ¿Qué veremos en esta guía?

**Sección 01.** Ciudadano Digital ..... **Pag. 04**

**Sección 02.** Derechos y responsabilidades en línea ..... **Pag. 05**

**Sección 03.** **SEGURIDAD EN LÍNEA**

Contraseña segura ..... **Pag. 08**

Autenticación ..... **Pag. 09**

Protección de la privacidad en línea ..... **Pag. 10**

Algunos tips prácticos ..... **Pag. 12**

**Sección 04.** **ETIQUETA EN LÍNEA Y RESPETO DIGITAL**

¿Cómo debemos comportarnos en línea? ..... **Pag. 16**

Prevención del ciberacoso ..... **Pag. 18**

**Sección 05.** **PARTICIPACIÓN CÍVICA EN LÍNEA**

¿Qué es la Clave Única y para qué sirve? ..... **Pag. 22**

Plataformas del Estado ..... **Pag. 22**

**Sección 06.** **COMPRADOR DIGITAL**

Bancarización ..... **Pag. 29**

¿Cómo utilizar una billetera digital prepago? ..... **Pag. 30**

**Sección 07.** Agradecimientos ..... **Pag. 31**



## CIUDADANO DIGITAL

### ¿QUE ES LA IDENTIDAD DIGITAL?

Cuando hablamos de ciudadanía digital, hacemos referencia a las habilidades y actitudes esenciales para que las personas pueden ejercer sus derechos digitales y participar activamente en la convivencia democrática, a través del uso de la tecnología y medios de comunicación de manera informada, segura, responsable y crítica, entendiendo que afecta e influencia en nuestras vidas y en la de otros.

**Para que logremos ejercer nuestra ciudadanía digital de una forma íntegra, debemos conocer y poner en práctica los siguientes conceptos:**





## **DERECHOS Y RESPONSABILIDADES EN LÍNEA**

Los derechos digitales empoderan a los individuos. Así mismo, las responsabilidades y la ética son cruciales para mantener un entorno digital saludable, en el entorno digital son fundamentales para garantizar una convivencia equitativa y segura en la sociedad moderna.



### **Derechos digitales:**

Son normas y reglas que regulan nuestro comportamiento en el ciberespacio, incluyendo los requerimientos básicos para desenvolvernosen éste, y que cumplen con la protección de datos, la ciberseguridad y la forma en que se usa la tecnología, promoviendo la libertad de expresión en el entorno digital.



### **Responsabilidad digital:**

Se refiere al conjunto de acciones éticas y prudentes que las personas deben asumir al interactuar en el entorno digital. Implica adoptar comportamientos que contribuyan a un uso seguro, respetuoso y ético de la tecnología y las plataformas digitales.



## EJEMPLOS DE DERECHOS DIGITALES

## ASPECTOS QUE INCLUYE LA RESPONSABILIDAD DIGITAL

### **Derecho a la privacidad y seguridad digital:**

Se refiere a la capacidad de controlar el uso, la recopilación y divulgación de la información personal que circula en línea, además de la protección de datos personales contra amenazas cibernéticas.

### **Ciberseguridad personal:**

Adoptar prácticas para proteger información personal y evitar ser víctima de delitos como robo de identidad o fraude cibernético.

### **Derecho al acceso universal a internet:**

Posibilidad de acceder a la conectividad en línea de manera equitativa y asequible.

### **Comportamiento ético:**

Mantener un comportamiento adecuado al interactuar con otros usuarios, evitando el ciberacoso, discursos de odio y otras conductas perjudiciales.

### **Derecho a la propiedad digital:**

Control sobre la propia información y contenidos digitales como fotos, archivos y datos.

### **Verificación de la información:**

Evaluar críticamente la veracidad de la información antes de compartirla en línea, previniendo así la propagación de la desinformación.

### **Derecho a la libertad de expresión digital:**

Libertad de expresar opiniones e ideas, teniendo la capacidad de convivir sin afectar la libertad de otras personas. No confundas libertad de expresión con odio.

### **Conformidad con Normativas y Términos de Servicio:**

Respetar las leyes y regulaciones en línea, además de cumplir con términos y condiciones establecidas por las plataformas digitales que se utilizan.

## SEGURIDAD EN LÍNEA



La seguridad es un aspecto crítico de la navegación en la web, ya que consiste en tomar medidas e interiorizar prácticas para proteger la información, los sistemas y a los usuarios en el entorno digital. Éste aspecto busca aminorar amenazas como: el robo de datos, ataques cibernéticos y fraudes electrónicos.



## Contraseñas seguras

Las contraseñas son combinaciones de caracteres, diseñadas para proteger el acceso a cuentas y sistemas. Se caracterizan por ser lo suficientemente complejas y únicas para evitar el intento de adivinanzas o ataques.

**Algunos aspectos que debes tener en cuenta para que tu contraseña sea segura son:**

### Longitud y complejidad



nombre23213@correo.cl



gr42sd85\_d12rTgw

- Utiliza contraseñas largas con al menos 12 caracteres.
- Prefiere usar combinaciones de letras mayúsculas, minúsculas, números y caracteres especiales.

### Evita información personal



maria1985@correo.cl



mar1985

- Evita usar información personal que fácilmente esté disponible, como nombres propios o de familiares, Rut, fecha de nacimiento, número de teléfono, dirección, etc.
- Evita secuencias obvias.

### Contraseñas únicas y actualización periódica



C0n7Ras3ña



m1g47e



r0d160

- Utiliza contraseñas únicas para cada cuenta. No reutilices contraseñas para todas tus redes o plataformas de servicios.
- Preocúpate de modificar tus contraseñas periódicamente, especialmente en cuentas sensibles o de mayor información como las del correo electrónico, banco, redes sociales, etc.



## Autenticación

La autenticación es el proceso de verificar tu identidad como usuario, para asegurar que tienes el permiso adecuado para acceder a un sistema o servicio, fortaleciendo así la seguridad de tus datos.

**Te recomendamos que lo apliques, así habrá más muros de protección a tus cuentas. Dentro de las opciones de autenticación encuentras las siguientes:**



### Autenticación de Dos Factores (2FA)

Es una capa adicional de seguridad que requiere una segunda forma de verificación de identidad más allá de la contraseña. Por ejemplo, para las transferencias en algunos bancos o algunas plataformas. Además de la contraseña o clave, se envía un código al número telefónico registrado para finalizar la transacción o acceso.



### Seguridad biométrica

Las funciones biométricas son aquellas como las huellas dactilares, reconocimiento facial o escaneo de iris, sin ingresar alguna contraseña o código.



### Monitoreo y registro

Se implementan sistemas de monitoreo y registro para realizar un seguimiento de los intentos de inicio de sesión y detectar actividades sospechosas a través de notificaciones.



## Protección de la privacidad en línea

La protección de la privacidad en línea se centra en salvaguardar la información personal de los usuarios mientras navegan en internet y servicios en línea. Involucra la implementación de uso de herramientas de cifrado para proteger los datos sensibles como lo son nombres, direcciones, número de teléfono, información financiera y cualquier otro dato que pueda identificar o vincular a una persona.

### Algunos ejemplos de cómo proteger la privacidad en línea:



**Navegación segura:** Utiliza conexiones seguras mediante **HTTPS** y evita conectarte a redes WI-FI públicas no seguras, especialmente, al realizar transacciones de dinero o ingresar información sensible.



**Mantener actualizados los dispositivos y aplicaciones:** Instalar regularmente actualizaciones de seguridad en tus dispositivos y aplicaciones para protegerlos contra vulnerabilidades conocidas.



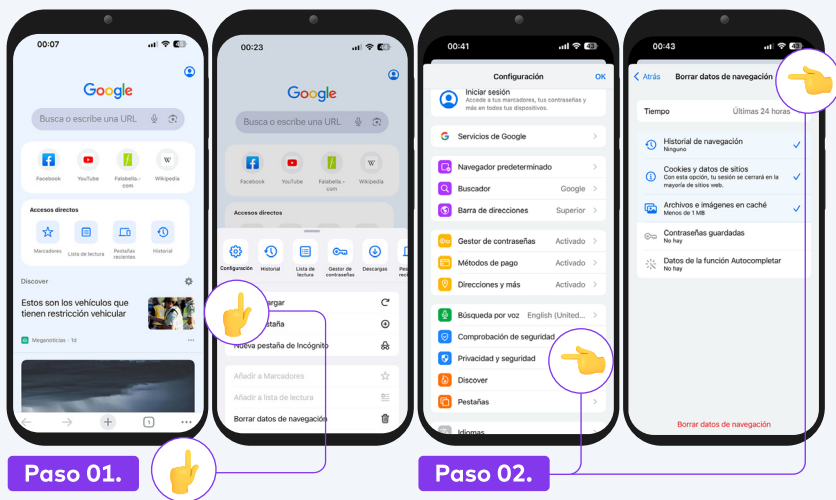
**Gestión de cookies y seguimiento:** Revisa y gestiona las cookies en tu navegador para controlar qué información se comparte con los sitios web.



**¡OJO!** Al aceptar las cookies de los sitios web que visitas te pueden llegar notificaciones de publicidad que no deseas, por esto es que debes leerlas antes de aprobar el acceso.

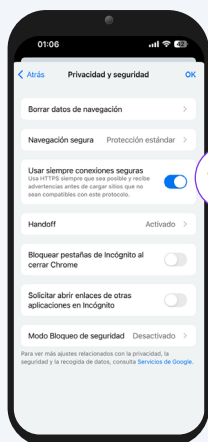
## Eliminación de cookies y configuración de sesiones

Eliminar las cookies de tu navegador es como hacer una limpieza profunda en tu espacio digital, asegurándote de que tu navegación por internet sea privada y segura. Piensa en las cookies como pequeñas notas que los sitios web dejan en tu dispositivo para recordarte. Aunque pueden ser útiles, acumular muchas de ellas puede afectar tu privacidad y la velocidad de tu navegador. Es como si cada sitio que visitas dejará un pequeño recuerdo en tu casa; con el tiempo, querrás ordenar y decidir qué conservar. Limpiar estas cookies regularmente te permite tomar el control de tu privacidad online, asegurándote de que solo compartes lo que deseas compartir. Te dejamos unos simples pasos para hacerlo en Google Chrome.



Abre tu aplicación y presiona los 3 puntos, en el panel debes buscar y presionar "Configuración".

Luego, debes presionar en "Privacidad y seguridad", después "Borrar datos de navegación", te aparecerá un listado de lo que puedes eliminar, cada cierto tiempo es recomendable eliminar el historial de navegación, las cookies y el caché. Luego de marcarlos presiona Borrar datos de navegación.



Además, en el apartado de configuración puedes activar el "Usar siempre conexiones seguras" donde recibirás advertencias antes de cargar una página que no cuente con el protocolo de HTTPS.



## Algunos tips prácticos

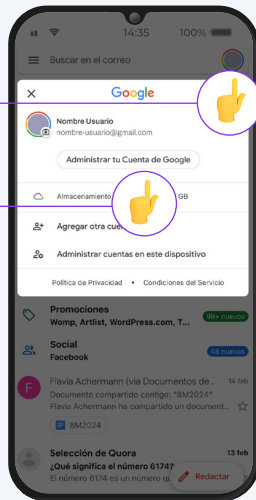
### Configuración de Autenticación 2FA

Activar la autenticación de dos pasos es como tener un doble cerrojo en tu puerta. Te brinda la seguridad de detectar y autorizar el acceso a tus cuentas desde dispositivos desconocidos. Hoy en día, la mayoría de aplicaciones y servidores de correo electrónico tienen esta función.

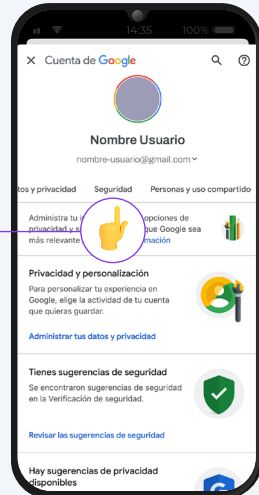
Al usar Redes Sociales o cualquier otro servicio en línea, asegúrate de iniciar y cerrar sesión correctamente, cuidando de tu espacio personal digital. Para activar la autenticación de dos pasos en tu correo Gmail sigue las indicaciones a continuación:

#### Paso 01.

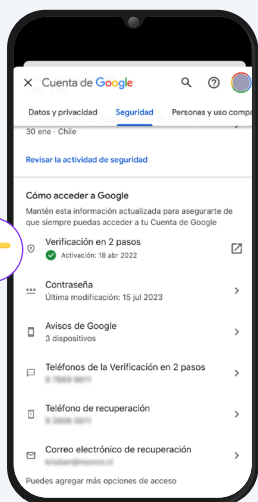
Dentro de tu correo electrónico, pulsa tu foto de perfil arriba a la derecha y accede a la opción "Administrar tu Cuenta de Google".



Selecciona la pestaña de "Seguridad".

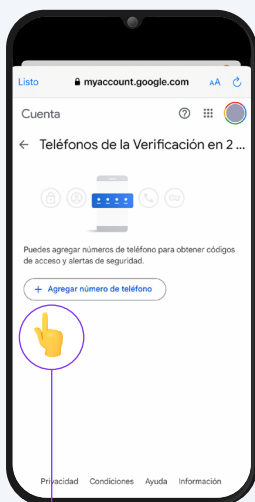






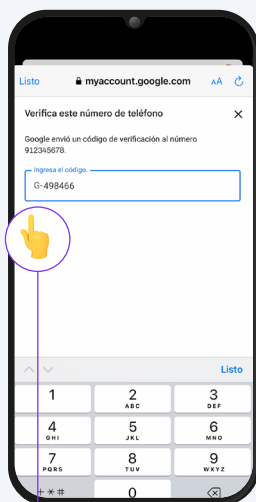
### Paso 02.

En la sección de "Seguridad", hacer clic en la opción "Verificación en dos pasos".



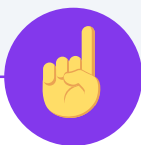
### Paso 03.

Te pedirá ingresar el número de teléfono para recibir los códigos de verificación.



### Paso 04.

Llegará un código a tu celular que debes poner en la casilla "Ingresar el código de verificación" para completar el proceso.



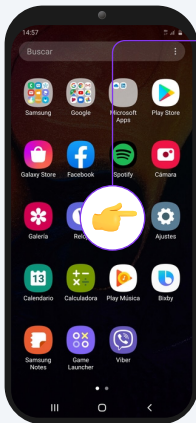
Considera que debes hacer este paso a paso desde tu correo abierto en un computador y tener a mano tu celular para completar el proceso.



No olvides proteger tus dispositivos con un buen antivirus, al igual que te proteges del sol con bloqueador. Y por último, guarda tus cosas importantes, como fotos y documentos, en la nube de internet; es como tener una caja fuerte para tus recuerdos y archivos importantes. ¡Sé un usuario inteligente y prevenido!"

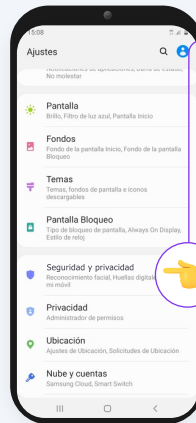
## Configuración de opciones de seguridad biométrica

Haz tu smartphone más seguro con solo un toque o una mirada. Activar la seguridad biométrica en tu teléfono es como añadir un guardián personal a tu dispositivo. Imagina que solo con tu huella digital o tu rostro, puedes darle a tu teléfono un nivel extra de protección, asegurando que solo tú puedas acceder a tus mensajes, fotos y aplicaciones. Esta función, disponible en la mayoría de los smartphones modernos, actúa como una barrera adicional contra intrusos, similar a tener una llave única para un tesoro que solo tú posees. ¿Lo mejor de todo?, es rápido y sencillo de configurar. Te dejamos el paso a paso de como activar la opción en un celular Android.



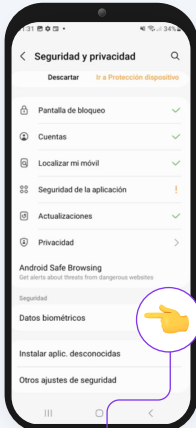
### Paso 01.

Ve a la aplicación "Configuración" en tu dispositivo Android



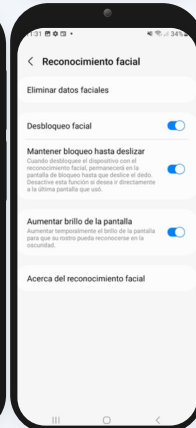
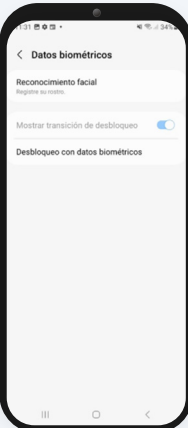
### Paso 02.

Busca alguna de estas opciones "Seguridad y privacidad", "Seguridad y ubicación", o simplemente "Seguridad". También puedes buscar en la lupa Q Datos biométricos.

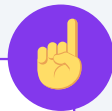


### Paso 03.

Busca la opción "Datos biométricos" y presionalo.



- Algunas aplicaciones pueden utilizar biometría para la autenticación.
- En el caso que tenga esa posibilidad puedes activar esta función dentro de la configuración de cada aplicación.
- Esta configuración puede variar de acuerdo a la marca y Sistema Operativo de tu Smartphone.



## ETIQUETA EN LÍNEA Y RESPETO DIGITAL



La interacción que tengamos en el mundo digital como redes sociales, chats, e-mails u otros debe ser similar a la que tenemos en la vida real. Por esto, debemos seguir reglas sociales básicas para respetar a las personas con quienes nos estamos comunicando. A lo anterior, se le nombra como **Netiqueta** o etiqueta en línea. Estas reglas no son algo normativo ni obligatorio, pero se deben cumplir para generar un ambiente apto para la comunidad digital.



## ¿Cómo debemos comportarnos en línea?

Te dejamos algunas recomendaciones que te pueden ayudar a reforzar las pautas a considerar para un buen comportamiento en línea. ¡Haz del internet un espacio seguro para todos y todas!



**Privacidad en la web:** A la hora de enviar información vía correo electrónico o realizar publicaciones fotográficas, opiniones u otros, solicita permiso antes de realizarlas, siempre debe haber un consentimiento por todas las partes involucradas más si es el caso de publicaciones que incorporen a menores de edad.



**Comunicación escrita y uso de medios sociales:** A pesar que la interacción en redes sociales es informal, considera cuidar tu ortografía y gramática, así generas mejor comprensión para las personas que reciben tus mensajes. Para el caso de correos electrónicos, la estructura es muy diferente a la de un chat. Si vas a expresar una opinión en la web, trata de manejarla con el mayor respeto.



**Comportamiento en medios sociales:** En redes sociales, debes entender que hay una persona tras cada perfil con sentimientos y vivencias, se consciente de tu huella digital y piensa antes de publicar comentarios ofensivos y/o información que puedan generar malos entendidos o desinformación.



**Normativas y políticas:** Intenta darte el tiempo leer las normativas de los medios en los cuales estás generando perfiles o cuentas, ya que estas reglas establecen límites y expectativas de tu comportamiento. Así evitarás sanciones, bloqueos de las cuentas u otras acciones por parte de los administradores por desconocimiento.



**Límites y tiempo en redes sociales:** Respeta los tiempos de los otros, se consciente que las personas no están todo el día leyendo u observando sus cuentas. Por otra parte, se consciente a la hora de enviar y responder mensajes o correos electrónicos. Si no cuentas con tiempo para leer, es recomendable que respondas que lo verás pronto.

Esperamos que estas recomendaciones te sirvan y puedas llevarlas a cabo, para convivir en un mundo digital ameno para todos.

## DEFINICIÓN NETIQUETA



**Privacidad  
en la web**



**Comunicación  
escrita y uso de  
medios sociales**



**Comportamiento  
en medios sociales**



**Normativas y  
políticas**



**Límites y tiempo en  
redes sociales**

## Prevención del ciberacoso



Existen personas que no cumplen con la netiqueta y muchas veces su objetivo es dañar a otras, por lo que incurren en acciones negativas hacia otros a través de internet, como en las redes sociales o directamente en teléfonos móviles con llamadas o mensajes. Si esto ocurre en reiteradas ocasiones, es acoso, nombrado también como ciberbullying o ciberacoso.

### ¿Cómo podemos identificar si estamos viviendo ciberacoso?



- Si alguien te envía mensajes insultándote, en reiteradas ocasiones.
- Si alguien te trata de amenazar o chantajear, diciendo que divulgará información tuya o enviará fotografías indebidas.
- Si dentro de un grupo online te eliminan sin razón, te excluyen y hablan mal de ti repetidamente. Asimismo, si rechazan tus intentos de comunicarte.

**Cybermobbing:**

Hostigamiento psicológico y maltrato a través de internet en el ámbito laboral.

**Grooming:**

Acoso de parte de un adulto a un menor, donde se engaña al menor para la extracción de material fotográfico.

**Cyberbaiting:**

Ocurre en el ambiente estudiantil, donde los alumnos se burlan de sus profesores.

**Frapping:**

La creación de perfiles falsos para publicar fotos, dañando tu reputación o la de otros.

**Cyberstalking:**

Es cuando una persona monitorea constantemente las publicaciones o el actuar de otra, a través de internet, siendo invasivo, afectando la privacidad y seguridad.

**Sextorsión:**

Es cuando se te amenaza en publicar material fotográfico o videos íntimos tuyos, si no cumples con lo que se te pide.

## ¿Cómo actúo ante estos sucesos?



No compartas ni des like a información u otro material que llegue a tus manos, si consideras que esto puede hacer daño a otra persona.

Si estás siendo acosado virtualmente, no estás solo en esto, busca apoyo de tus cercanos de confianza.

No hables, ni respondas a la persona que te acosa.

Guarda evidencia a través de pantallas de chats, mails o mensajes.

Todas las redes sociales tienen la opción de reportar contenido inadecuado en publicaciones o bien bloquear los perfiles.

Si te sientes amenazado y en peligro, denuncia a las autoridades. En Chile, la Unidad de Cibercrimen de la Policía de Investigaciones es la encargada de asesorar en estos casos y cuenta con un número de  WhatsApp +569 3459 9762.

\*En caso que ocurran estos sucesos en una comunidad estudiantil, se debe ingresar a la **Superintendencia de Educación**.

Superintendencia  
de Educación



[www.supereduc.cl](http://www.supereduc.cl)

¡Solicita apoyo y denuncia!



Para mayor información **ingresa al sitio gubernamental de violencia digital** y te invitamos a leer con precaución la Ciberguía de Denuncia al Abuso Digital que indica el paso a paso de cómo reportar perfiles y hacer denuncias.

[www.gob.cl/saludablemente/violenciadigital](http://www.gob.cl/saludablemente/violenciadigital)



**PARTICIPACIÓN  
CÍVICA EN LÍNEA**



**La Clave Única** es el medio de acceso a los servicios del Estado de manera fácil y segura. Es personal e intransferible y te permite realizar trámites a través de las plataformas gubernamentales. Como sabemos, además de tener nuestro correo electrónico que nos identifica en la web, nuestro Run y Clave Única son esenciales para hacer trámites digitales y se deben resguardar, no debes compartirla.



**¿Quiénes pueden acceder a ella?**

Cualquier persona mayor de 14 años puede hacer válida su Clave Única, solo necesita su cédula de identidad y un correo electrónico. ¿Quiénes pueden acceder a ella?

## Pasos para obtener Clave Única:

Solicítala vía telemática, solicitando una hora de videoconferencia <https://codigo.srcei.cl/> o bien presencialmente en oficinas del Registro Civil.

Actívala: Te harán entrega de un código de activación, el cual tendrás que ingresar en el siguiente link: <https://claveunica.gob.cl/activar>

Listo, ya podrás acceder a cualquier sitio gubernamental para efecto de trámites que debas realizar.



Para mayor información ingresa a la página <https://claveunica.gob.cl/>

 o bien llama al **600 360 33 03**



## Plataformas del Estado

Como principio fundamental, las y los ciudadanos debemos acceder a los servicios del Estado, podemos hacerlo de manera online, permitiendo así la agilidad en los procesos y mejorar la calidad de vida en el ahorro de tiempo y dinero.

### ¿Qué es Chile Atiende?



Dentro de las plataformas más importantes de realización de trámites del Estado está Chile Atiende, una red multiservicios que alberga la mayor información respecto a los trámites que deseas saber o realizar.

### ¿Cómo funciona?

Posee distintos canales de atención en línea:

Sitio web:

[www.chileatiende.gob.cl](http://www.chileatiende.gob.cl)

Redes sociales:



Facebook



Instagram



X

(exTwitter)

También puedes llamar al número  **101**, o bien acudir presencialmente a una de las 190 oficinas que se encuentran a nivel nacional.



### Naveguemos por la plataforma

.01

### Ingresa al sitio web de Chile Atiende

Es similar a cualquier navegador y tiene una barra buscadora de trámites. Aquí vamos a buscar un Certificado de Nacimiento, que es el trámite más común.

Escribe en la barra, el trámite que necesites. En donde dice ¿Qué estás buscando?. Te arrojará distinta información referente a esto. Elige la opción que corresponda.



.02

## Rellena la ficha

Chile Atiende arroja una ficha que tiene los siguientes apartados: **descripción, a quién va dirigido, costos, qué necesito para hacer el trámite y botón de descarga o ir al trámite.**

**Ojo:** Algunos trámites online son gratuitos. Ten en cuenta esto antes de dirigirte presencialmente, así ahorrarás tiempo de traslado y dinero.

### Certificado de nacimiento

Última actualización: 23 de enero, 2024

At A:

#### Descripción

Acredita número de inscripción, nombre, RUN, registro, además de la fecha y lugar de nacimiento de una persona.

Existen tres tipos:

- Todo trámite.
- Asignación Familiar.
- Matricula.

Obtén tu certificado

Conocer más

Costo del documento

Conocer más

▼ Descargar certificado



¿Tienes dudas con este trámite?

Comunícate con nosotros:



Haz clic en el botón de descargar certificado, te derivará a la página del Registro Civil.



### Certificados en línea

Estimado(a) usuario(a), con el fin de proteger sus datos personales, para la obtención de certificados de nacimiento, matrimonio y/o defunción, se requerirá el RUN y el Número de Documento del solicitante, de conformidad con la ley 19678, sobre protección de la vida privada.

▼ Más solicitados

- Certificado Nacimiento Para Asignación Familiar
- Certificado Antecedentes Fines Particulares
- Certificado de Matrimonio Para Asignación Familiar

- > Nacimiento
- > Matrimonio
- > Defunciones
- > Antecedentes
- > Vehículos
- > Prendas
- > Profesionales

Carro de Certificados

Total \$ 0

Detalle

Su cargo #112 veces.

.03

Selecciona el certificado e ingresa los datos correspondientes, si el documento lo debes presentar en el extranjero, debes apostillarlo. Considera el pago con tarjeta de ser necesario.

.04

Finalizando te confirmará el envío a tu correo adjuntando el documento y ¡listo! Ya lo podrás usar para lo que necesites.



### ¿Eres Migrante o estás de paso en nuestro país?

Si la respuesta es sí, encuentre la información que necesites en el **sitio web del Servicio Nacional de Migraciones**.

### ¿Qué es el Servicio Nacional de Migraciones?

Es la institución encargada de garantizar que los procesos migratorios sean seguros y ordenados para cumplimiento de la legislación migratoria. Tiene oficinas a nivel nacional.

Al acceder a esta página, podrás obtener información de los requisitos y trámites migratorios.

- Trámites Digitales — Ir a trámites digitales.
- Ayuda Migraciones
- Reserva tu hora — Agenda hora para asistir presencial

Para hacer de manera online tu diligencia, debes acceder a través de tu Clave Única o bien hacer una cuenta en el sitio web.

Si no cuentas con Clave Única, créate una cuenta en el **Servicio Nacional de Migraciones aquí**



Crear cuenta

Iniciar sesión

Iniciar con ClaveÚnica



Una vez obtenida tu cuenta, podrás acceder al Portal de Trámites Digitales.

Aquí encontrarás: Trámites de residencia definitiva, trámites de nacionalización, solicitud de visas, trámites turistas, entre otros.



**Te dejamos aquí otros lugares de relevancia a la hora de acudir a información de trámites migratorios:**



Si deseas hacer una consulta general, ingresa al **Sistema de Atención Ciudadana** aquí.



Si deseas saber información de las oficinas a nivel nacional, ingresa aquí.



Para agendar hora presencial de atención ingresa aquí.



**COMPRADOR  
DIGITAL**



Se refiere a una persona que realiza compras en línea usando plataformas digitales, como sitios web de comercio electrónico, aplicaciones móviles o redes sociales. Ser un comprador digital implica estar familiarizado con el uso de herramientas digitales y tener confianza en la seguridad y conveniencia de las transacciones en línea.

Algunos aspectos muy importantes que debes tener en cuenta para comprar en internet:



**Seguridad en línea:** Verifica que la URL comience con **https://** y busca un candado  en la barra de direcciones del navegador.



**Reseñas y comentarios:** Antes de realizar una compra, lee las reseñas y comentarios de otros usuarios sobre el producto y/o el vendedor, para tener claridad de su calidad y confiabilidad.



**Comparación de precios:** Compara precios de diferentes sitios web para asegurarte de obtener la mejor oferta posible. Un ejemplo de plataforma es: knasta, donde podrás ver el historial de precios del producto durante periodos de tiempo, para tomar la mejor decisión.



**Pago:** Considera tener tus tarjetas débito o crédito cerca, para que puedas realizar el pago de tus productos o servicios. Los datos de tus tarjetas no deben ser compartidos con otras personas. Asegúrate de no guardar estos datos en los navegadores.



**Seguimiento y entrega:** Verifica las opciones de entrega disponibles y el tiempo estimado de llegada del producto. Además, asegúrate de poder rastrear tu pedido para seguir su proceso hasta que llegue a tu ubicación.



## Bancarización:

La bancarización es importante en el contexto de las compras digitales porque proporciona a los compradores acceso a servicios financieros que permiten realizar pagos en línea de manera segura y conveniente. Además, ayuda a la inclusión financiera, al darle acceso a servicios bancarios a las personas que no tienen acceso a ellos.

Respecto a los métodos de pago en las compras digitales, estos varían dependiendo del país y de la plataforma del comercio electrónico, pero los métodos más comunes son:



**Tarjeta de crédito y débito:** Los usuarios deben ingresar los detalles de su tarjeta de crédito o débito directamente en el sitio web de compra para realizar el pago, siguiendo las instrucciones.

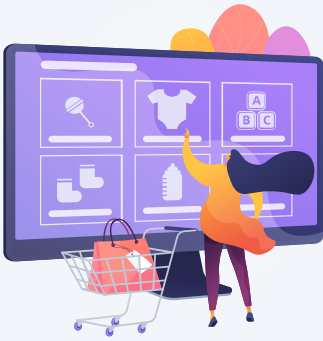


**PayPal:** Servicio de pago en línea que permite a los usuarios enviar pagos de forma segura a través de internet. Los usuarios deben vincular su tarjeta de crédito o débito a la cuenta PayPal para realizar pagos en línea de forma rápida y segura, sin ingresar los datos una y otra vez en diferentes plataformas.



**Billeteras digitales:** Son aplicaciones móviles que permiten a los usuarios almacenar dinero en una tarjeta digital, se puede acceder a tarjetas de débito y crédito. Se pueden realizar pagos y transacciones en línea de manera rápida y conveniente. Ejemplos de algunas aplicaciones: Mercado Pago, MACH, Tenpo, etc.

**Con las billeteras digitales puedes pagar tus plataformas de streaming y servicios básicos, como luz, agua, gas (por aplicación), etc.**



## ¿Cómo utilizar una billetera digital prepagó?

Imagina una billetera digital como una versión moderna de tu billetera física, pero en tu dispositivo móvil. Funciona como un lugar seguro donde puedes almacenar dinero que has cargado previamente.

.01

**Descarga la aplicación:** Busca en la tienda de aplicaciones de tu teléfono y descarga la aplicación de la billetera digital que deseas usar.

.02

**Regístrate:** Abre la aplicación y sigue las instrucciones para registrarte. Es posible que necesites proporcionar algunos detalles personales básicos.

.03

**Carga dinero:** Una vez registrado, puedes cargar dinero en tu billetera digital desde tu cuenta bancaria o mediante otros métodos de pago.

.04

**Usa tu billetera:** Puedes usarla para hacer compras en línea o en tiendas físicas donde se acepten pagos digitales. Solo necesitas abrir la aplicación y escanear un código QR o ingresar tu información de pago.

.05

**Controla tus gastos:** La aplicación de la billetera digital te permite llevar un registro de tus transacciones y controlar tus gastos. Puedes ver cuánto dinero tienes disponible en todo momento.

.06

**Recarga cuando sea necesario:** Si te quedas sin dinero en tu billetera digital, puedes recargarla fácilmente desde tu cuenta bancaria u otros métodos de pago. Es como recargar saldo en tu teléfono móvil.

¡Listo! Ya estás preparado para comenzar a utilizar tu billetera digital prepagó y realizar pagos, enviar dinero a amigos y familiares, hacer compras en línea y mucho más. Recuerda revisar los términos y condiciones de estas billeteras.



# ¡Gracias!

Fundación País Digital agradece tu participación en nuestras capacitaciones de Alfabetización Digital. Para nosotros es importante continuar aportando al desarrollo económico y la disminución de la brecha digital en Chile, transmitiendo los contenidos de forma adaptada y cercana a su contexto y realidad. Gracias por ser parte.

Les saluda:

**Unidad de desarrollo digital  
Programa Conectando Territorios | Fundación País Digital 2024**



# Ciudadano Digital

Este documento busca entregar información general sobre herramientas digitales, todas las paginas y marcas son referenciales, se excluye de cualquier responsabilidad a los autores en el uso de estas. La disponibilidad de los servicios se encuentra restringida según el lugar geográfico en donde se encuentre el lector.

Todos los derechos reservados © País Digital 2024.

Este trabajo tiene licencia abierta a través de CC BY-NC-ND 4.0.